sysadmin

Posted by u/imwearingatowel 6 days ago

18

dmarcian Data Breach?

Woke up to a long-winded and somewhat confusing email from dmarcian <securityofficer@dmarcian-europe.com> today, claiming they suffered some type of data breach.

The full email is way too long to include here, so I've put it on pastebin: https://pastebin.com/tkPVrAyL

> Dear customer of dmarcian Europe BV,
>
> Recently we had to inform many of our users and the Dutch Data Protection Authority of a data breach caused by dmarcian, Inc. As a result of the breach we have launched a new and dedicated European instance with the dmarcian application which is securely under our control. Although we do not yet have control of all historic data, the impact of the data breach is now more and more limited.

I can't really decipher what actually happened from the email, and if it was an actual cybersecurity breach or some legal dispute between the US and EU divisions of the company.

Has anyone heard more about this, or can validate/comment on any of the claims they're making? We never received any of the previous emails referenced in today's email.

The email goes on to ask us to set up a new account on a new, dedicated EU platform...

The whole thing smells off.

Exhibit E

dmarcian

Edit this banner >>

DMARCian EU data breach

B **bill** 4d

What is the meaning of the post here: Dmarcian.eu 10

I received a confusing e-mail with nearly the same content. They are asking me to change the DNS of all my domains on the European instance. My domains on other instances can be accessed normally.

What's going on?

Reply

created	last reply	replies	views	users	likes	links
B 4d	U 1d	6	129	4	8	2

This is the first time 4nd3r5 has posted — let's welcome them to our community!

4nd3r5 3d

I totally agree.
I haven't got an email, but this is very confusing and very unprofessional.
My account has been on dmarcian.eu, and has now been moved to eu.dmarcian.com.
It seems like the group behind dmarcian.eu seems to think there has been a data breach.
Please find a common ground as quickly as possible, this is bad for everyone.

Reply

dmarcian customers are serviced through *dmarcian.com* and customers should be suspicious of anyone or any service pushing their business and their data away from our trusted *dmarcian.com* domain.

Always check the URLs of where you and your data are being directed to. All legitimate dmarcian communications and service will come from *dmarcian.com* in all other regions as well.

Other sites are NOT associated with *dmarcian.com* and therefore, do not have the rights to use our brand or sell our services

2 Reply Share Save Edit •••

lirettype 3 days ago

So as a customer, who created his account on dmarcian.eu, who owns what? And worse, who am I sending my dmarc data to, right now?

3 Reply Give Award Share Report Save

dmarcianCEO 2 days ago

Please contact me at brand-abuse@dmarcian.com and I can help you find these answers regarding your account.

2 Reply Share Save Edit •••

imwearingatowel 2 days ago

This whole situation has been handled absolutely horribly, by both parties. This situation should be dealt with privately in the courts. Instead, you're dragging your customers into the fight, like mommy and daddy fighting in front of the kids during a divorce.

All of this has completely eroded any faith we have in dmarcian (US and EU). We'll be moving to a new provider.

2 Reply Give Award Share Report Save

emailsecuritygeek 1 day ago

We moved to OnDMARC if you're interested in checking them out

3 Reply Give Award Share Report Save

Annalisa 9:13 AM

Yesterday

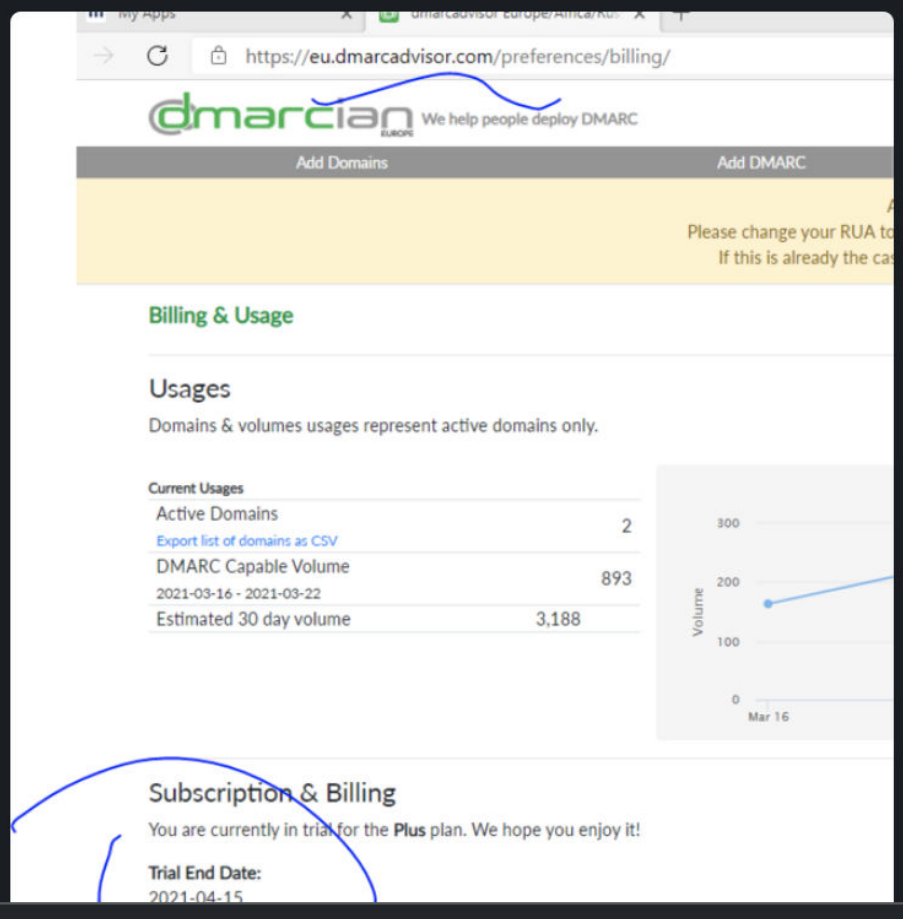
```
Unfortunately, I had to change my DMarc record twice during
the trial and so have not yet gained any useful data
I contacted support who said they would extend the trial. I
assume that didn't happen?
```

Gentleman emailed me at EoT regarding an extension he requested through support. No one on our side had seen a request, so I asked who he contacted.

```
Hello. Sorry I don't know
However, the trial now shows end date of 15/4/2021 so all is
good
```

he included this screenshot showing the BV site he is accessing.
https://dmarcian.pipedrive.com/deal/64161

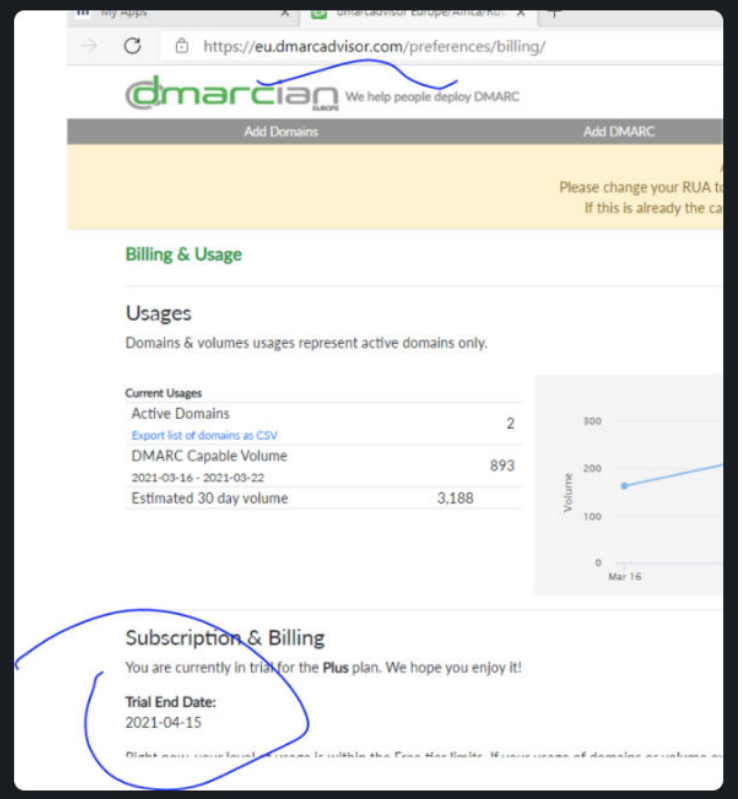
image.png



Message #advisorresponse

161

image.png



2 replies

Ben 5 hours ago

here we should reach out saying something like: 'please be aware that you are NOT on dmarcian.com. Instead you have been signed up to a platform called dmarcadvisor.com. If this was your intention, all is ok.
If you wanted and expected to have an account on dmarcian.com please let us know.'
I have a similar situation with a partner who just signed with EU a few weeks ago and had the impression (and also wanted) to work with dmarcian.com. Nobody from EU pointed out the difference. Now they want to switch to us.

Tomki 🔥 1 hour ago

Trustpay "Since 11.3. we do not see any DMARC data in our console. Could you please verify what could be the problem?"
Rapha Racing "Subject: **All my data is gone**

```
I am in the EU region.
My Domain Overview shows now data for the last 7 days
however the DMARC validator shows my DMARC records for RUA
etc as being correct
and the DataReporters shows reports received up until
today.
What has gone wrong ?
Do I need to start using the dmarcian.eu website now ?"
```

Shannon 🗒️ 1 hour ago

What? where are they signing in from?
As far as the letter. The lawyers are working on that content and will have that to us after the file the Temporary Restraining Order agains the BV today or tomorrow,

New

Tomki 🔥 1 hour ago

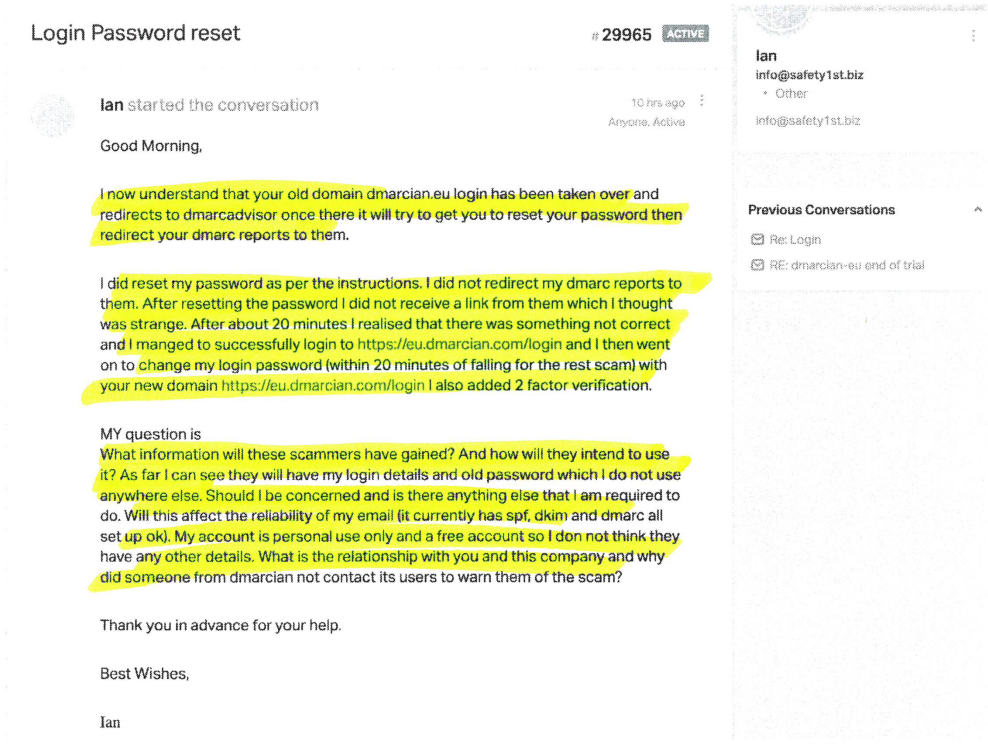
Rapha racing: The ticket was submitted via our in-app support page, so they're using the correct site.

- they're a basic-chargebee EU account
- They followed the illicit advice and have reporting changed to dmarcadvisor.com.
- the domain Overview DMARC record indicator is green(it's a validly formatted DMARC record), and so is the output from our other DMARC tools.

Pamela Duffy

Subject: FW: customer reaction messaging
Attachments: Screen Shot 2021-03-19 at 11.17.40.png

-------- Forwarded Message --------
Subject:customer reaction messaging
Date: Fri, 19 Mar 2021 11:16:37 -0700
From: Tomki Camp <tomki@dmarcian.com>
To: Shannon Draegen <shannon@dmarcian.com>



Login Password reset # 29965 ACTIVE

Ian started the conversation 10 hrs ago
Anyone, Active

Good Morning,

I now understand that your old domain dmarcian.eu login has been taken over and redirects to dmarcadvisor once there it will try to get you to reset your password then redirect your dmarc reports to them.

I did reset my password as per the instructions. I did not redirect my dmarc reports to them. After resetting the password I did not receive a link from them which I thought was strange. After about 20 minutes I realised that there was something not correct and I manged to successfully login to https://eu.dmarcian.com/login and I then went on to change my login password (within 20 minutes of falling for the rest scam) with your new domain https://eu.dmarcian.com/login I also added 2 factor verification.

MY question is
What information will these scammers have gained? And how will they intend to use it? As far I can see they will have my login details and old password which I do not use anywhere else. Should I be concerned and is there anything else that I am required to do. Will this affect the reliability of my email (it currently has spf, dkim and dmarc all set up ok). My account is personal use only and a free account so I don not think they have any other details. What is the relationship with you and this company and why did someone from dmarcian not contact its users to warn them of the scam?

Thank you in advance for your help.

Best Wishes,

Ian

Ian
info@safety1st.biz
• Other
info@safety1st.biz

Previous Conversations
Re: Login
RE: dmarcian-eu end of trial

Gj (gerrit) Jansen started the conversation

Mar 16, 2:30
Anyone, Active

Dear sir/madam,

Achmea Interne Diensten N.V. Zeist, Netherlands has a DMARCIAN subscription Enterprise contract since September 1, 2020. With Quotation number 1996 / v1. Unfortunately, we now see that access to the API has been blocked. We require you to regain access to the API as this is part of the concluded contract. We trust that you will make the API and all other services freely accessible and available again soon as was previously the case.

Kind regards,

Achmea IT | S&G IT Security Scanning & Engineering
Gerrit Jansen

Laan van Malkenschoten 20 | 7333 NP Apeldoorn
Postbus 9150 | 7300 HZ Apeldoorn
Aanwezig op maandag, dinsdag, woensdag, donderdag

Khadija.el-Attar-Sofi@renault.com started the conversation

Mar 17, 7:36
Anyone, Active

To: ernest@dmarcian.com, ben.vdi@dmarcian.com, ton@dmarcian.com
Cc: support@dmarcian.com, ancelin.schoenhentz@renault.com, charles.bruneteau@renault.com

Dear dmarcian Inc team,

On the 15th of March 2021 we were notified of a conflict involving dmarcian Inc. and dmarcian BV, which strongly impacted our relations that started in November 2019 with dmarcian BV.
Due to the risks we are now exposed to in terms of data protection regulations, we require from you to delete all data and reports concerning the Renault account without delay and no later than 26/03/2021.
We expect you to confirm in writing that the deletion has been completed (on the main servers and any backups and/or archives).

Best regards,

Cordialement,

Khadija EL ATTAR SOFI
http://group.renault.com/RCW_BINARIES/signature_renault/EMAIL_LOGOS_Groupe_Renault.png

DI-RS - Sécurité Informatique IS/IT
API : FREQVNOV352
13, Av Paul Langevin
92359 Le Plessis Robinson CEDEX
www.groupe.renault.com

sktransport.co.uk #29972 ACTIVE

Lesli Speers started the conversation 3 hrs ago

Anyone, Active

Hi

Can you tell me why there has been no DMARC reports on my domain for the past week?

Kind regards

Lesli

Lesli Speers

MSc BSc (Hons) MCIHT MCILT

Director

SK

Please click here for our current COVID-19 policy

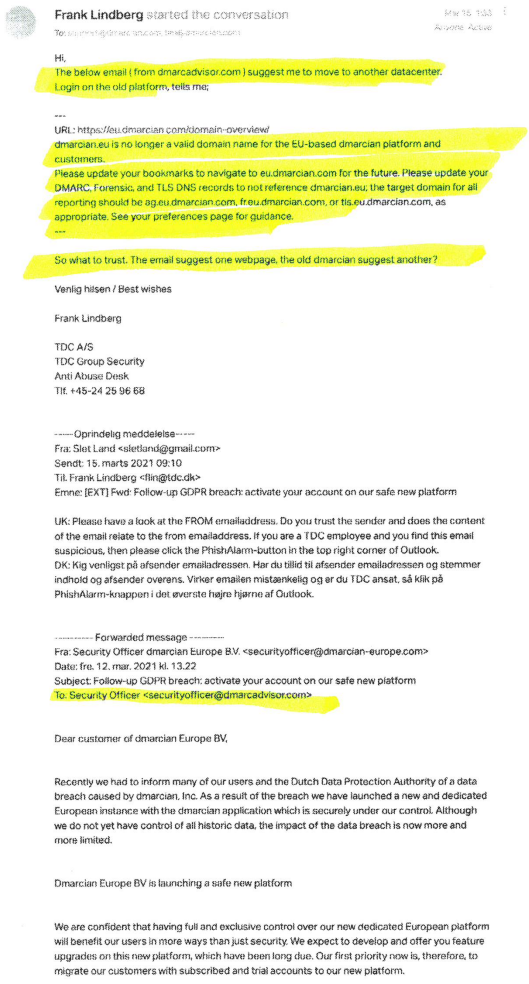
SK Transport Planning Ltd

Albion Wharf, Manchester, M1 5LN

07809 876 704

ls@sktransport.co.uk

sktransport.co.uk



Frank Lindberg started the conversation

Hi,
The below email (from dmarcadvisor.com) suggest me to move to another datacenter.
Login on the old platform, tells me;

URL: https://eu.dmarcian.com/domain-overview/
dmarcian.eu is no longer a valid domain name for the EU-based dmarcian platform and customers.
Please update your bookmarks to navigate to eu.dmarcian.com for the future. Please update your DMARC, Forensic, and TLS DNS records to not reference dmarcian.eu; the target domain for all reporting should be ag.eu.dmarcian.com, fr.eu.dmarcian.com, or tls.eu.dmarcian.com, as appropriate. See your preferences page for guidance.

So what to trust. The email suggest one webpage, the old dmarcian suggest another?

Venlig hilsen / Best wishes

Frank Lindberg

TDC A/S
TDC Group Security
Anti Abuse Desk
Tlf. +45-24 25 96 68

-----Oprindelig meddelelse-----
Fra: Slet Land <sletland@gmail.com>
Sendt: 15. marts 2021 09:10
Til: Frank Lindberg <flin@tdc.dk>
Emne: [EXT] Fwd: Follow-up GDPR breach: activate your account on our safe new platform

UK: Please have a look at the FROM emailaddress. Do you trust the sender and does the content of the email relate to the from emailaddress. If you are a TDC employee and you find this email suspicious, then please click the PhishAlarm-button in the top right corner of Outlook.
DK: Kig venligst på afsender emailadressen. Har du tillid til afsender emailadressen og stemmer indhold og afsender overens. Virker emailen mistænkelig og er du TDC ansat, så klik på PhishAlarm-knappen i det øverste højre hjørne af Outlook.

---------- Forwarded message ---------
Fra: Security Officer dmarcian Europe B.V. <securityofficer@dmarcian-europe.com>
Date: fre. 12. mar. 2021 kl. 13.22
Subject: Follow-up GDPR breach: activate your account on our safe new platform
To: Security Officer <securityofficer@dmarcadvisor.com>

Dear customer of dmarcian Europe BV,

Recently we had to inform many of our users and the Dutch Data Protection Authority of a data breach caused by dmarcian, Inc. As a result of the breach we have launched a new and dedicated European instance with the dmarcian application which is securely under our control. Although we do not yet have control of all historic data, the impact of the data breach is now more and more limited.

Dmarcian Europe BV is launching a safe new platform

We are confident that having full and exclusive control over our new dedicated European platform will benefit our users in more ways than just security. We expect to develop and offer you feature upgrades on this new platform, which have been long due. Our first priority now is, therefore, to migrate our customers with subscribed and trial accounts to our new platform.

--
Tomki Camp
Service Director
tomki@dmarcian.com

--
Shannon Draegen
CEO | dmarcian.com
shannon@dmarcian.com

marco.foglio@4wardpro.it started the conversation

40 mins ago
Anyone, Active

A user has submitted a **question**.

User Information

User ID	**19477**
User e-mail address	**marco.foglio@4wardpro.it**
Account ID	**7689**
Account	**Progel SpA**
Tier	enterprise
Subscription	subscriber
Partner	Yes
Region	**eu**
Origin page	**/domain-overview/**

Question

Subject: **DMARCIAN EUROPE B.V vs DMARCIAN INC**

```
Dear support,
I wanted to ask for some information about the legal dispute between DMARCIAN EUROPE
B.V and DMARCIAN INC.
It is unclear whether our subscriptions are still valid and which company we are payi
ng the bills to.
Now we are confused because we feel like we have customer data on both platforms
We would also like to understand for new European customers what information to give
for these issues:
1.      In which datacenter is the data present and from which internet provider is m
anaged by?
2.      which company is the data owner
or more generally what are your compliance policies for the EU GDPR?

Thanks in advance for your cooperation
```